## Abstract

A method and computer operated software application for digitally signing a portion of an electronic file, and for verifying such a digital signature. A portion of the file to be signed is extracted based on a computation of one or more functions, and the file portion is used for being either directly digitally signed, or for calculating a Message Digest value (MD1) and for digitally signing the MD1 value with a private key of the signer. The so-formed digital signature is appended to the file. During verification, the digital signature is removed from the file, decrypted using the signer's public key, which is known to the verifier, and the portion of the file, or respectively MD1 is obtained. The portion of the file used for the signature is again obtained and used for a similar a computation based on the one or more functions, which are also known to the verifier, for calculating a corresponding portion of the file, or another Message Digest value (MD2). MD1 and MD2 are compared, or alternatively the file portions are compared, to determine the authenticity and integrity of the file.